

4/5/1 (Item 1 from file: 351)

DIALOG(R)File 351:DERWENT WPI

(c) 2000 Derwent Info Ltd. All rts. reserv.

009932868 **Image available**

WPI Acc No: 94-200579/199424

Related WPI Acc No: 94-177433

XRPX Acc No: N94-157736

Security maintaining method for communication units using encryption - holding encrypted keys in non volatile memory and decoding them on power up with tamper detection circuit causing erasure of keys when tampering is detected

Patent Assignee: MOTOROLA INC (MOTI)

Inventor: BERGUM R A; VAN BOSCH J A

Number of Countries: 002 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9413080	A1	19940609	WO 93US10914	A	19931110	H04L-009/00	199424 B
EP 671090	A1	19950913	WO 93US10914	A	19931110	H04L-009/00	199541
			EP 94908563	A	19931110		
US 5457748	A	19951010	US 92983182	A	19921130	H04L-009/08	199546
JP 8504067	W	19960430	WO 93US10914	A	19931110	H04L-009/00	199645
			JP 94513184	A	19931110		

Priority Applications (No Type Date): US 92983182 A 19921130

Cited Patents: US 4605820; US 4723283; US 4849927; US 4888802; US 4924513;

US 4926475; US 4934846; US 5081675; US 5131040; US 5150412; US 5222136;

US 5241597

Patent Details:

Patent	Kind	Lan	Pg	Filing	Notes	Application	Patent
WO 9413080	A1	E	21				
EP 671090	A1	E	21	Based on		WO 9413080	
US 5457748	A		7				
JP 8504067	W		18	Based on		WO 9413080	

Abstract (Basic): WO 9413080 A

The encryption algorithm requires a key for operation and this is held in RAM (105) for normal use. The key is also encrypted and held in EEPROM (106). When powering down the RAM keys are overwritten. On power up, the EEPROM key is decrypted and stored in RAM. If tampering is detected (108) the EEPROM key is altered.

The appts has receiver (101) and transmitter (102) units connected to a microcontroller (103). This handles digitised data (109,110) and applies an encryptor (104) and a decryptor to the data.

USE/ADVANTAGE - E.g. for in-car mobile portable radios. Improves security of encryption key by encoding it and destroying it when tampering is detected.

Dwg.1/3

Title Terms: SECURE; MAINTAIN; METHOD; COMMUNICATE; UNIT; ENCRYPTION; HOLD; ENCRYPTION; KEY; NON; VOLATILE; MEMORY; DECODE; POWER; UP; TAMPER; DETECT ; CIRCUIT; CAUSE; ERASE; KEY; TAMPER; DETECT

Derwent Class: W01; W02

International Patent Class (Main): H04L-009/00; H04L-009/08

International Patent Class (Additional): G09C-001/00; H04L-009/10;

H04L-009/12

File Segment: EPI

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平8-504067

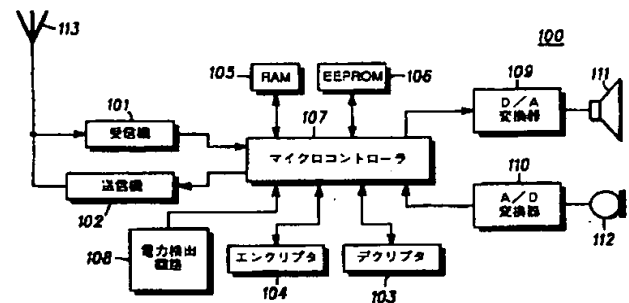
(43) 公表日 平成8年(1996)4月30日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I
H 0 4 L 9/00			
G 0 9 C 1/00		7259-5 J	
H 0 4 L 9/10			
9/12			
		8842-5 J	
			H 0 4 L 9/00 Z
			審査請求 未請求 予備審査請求 有 (全 18 頁)
(21) 出願番号	特願平6-513184		
(86) (22) 出願日	平成5年(1993)11月10日		
(85) 翻訳文提出日	平成7年(1995)5月26日		
(86) 国際出願番号	PCT/US93/10914		
(87) 国際公開番号	WO94/13080		
(87) 国際公開日	平成6年(1994)6月9日		
(31) 優先権主張番号	07/983, 182		
(32) 優先日	1992年11月30日		
(33) 優先権主張国	米国 (US)		
(81) 指定国	EP (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, M C, NL, PT, SE), J P		
(71) 出願人	モトローラ・インコーポレイテッド アメリカ合衆国イリノイ州60196シャンパ ーグ、イースト・アルゴンクイン・ロード 1303		
(72) 発明者	パーガム, ルセル・エー アメリカ合衆国イリノイ州レイク・ズリッ チ、アスペン・コート1034		
(72) 発明者	バン・ボスチェ, ジェームス・エー アメリカ合衆国イリノイ州クリスタル・レ イク、ブルー・バイン・ドライブ2015		
(74) 代理人	弁理士 本城 雅則 (外1名)		

(54) 【発明の名称】 暗号化通信装置内の改善された機密性に関する方法および装置

(57) 【要約】

デジタル暗号化を利用する通信装置内で、暗号化キーを暗号化されない形および暗号化された形でそれぞれ格納するために、揮発性メモリおよび不揮発性メモリが用いられる。電力検出回路が干渉検出回路構成と共に用いられ、非機密動作条件の場合に揮発性メモリからキーを積極的に消去できるようにする。



【特許請求の範囲】

1. 送信機と、受信機と、前記送信機を介して送信される情報を暗号化する暗号化手段と、前記受信機により受信される情報の暗号解読を行う暗号解読手段と、前記暗号化手段および前記暗号解読手段によって用いられ、それぞれ情報を暗号化および暗号解読する少なくとも1つのキーとを有する通信ユニットにおいて、前記少なくとも1つのキーの機密性を維持する改善された方法であって：

a) 前記少なくとも1つのキーの暗号化表現を不揮発性メモリに格納する段階；

b) 前記通信ユニットの電源投入時に、前記暗号解読手段により前記少なくとも1つのキーの暗号化表現の暗号解読し、前記少なくとも1つのキーを再構成する段階；

c) 前記少なくとも1つのキーを揮発性メモリに格納する段階；

d) 処理回路により、非機密動作条件を検出する段階；

および

e) 前記非機密動作条件を検出すると、前記少なくとも1つのキーを前記揮発性メモリから消去する段階；

によって構成されることを特徴とする方法。

2. 段階（d）が前記通信ユニットに対する電源の遮断を前記非機密動作条件として検出する段階によってさらに構成される請求項1記載の方法。

3. 段階（d）が前記少なくとも1つのキーに対する不当な方法によるアクセスが試みられていることを検出する段階によってさらに構成される請求項1記載の方法。

4. 前記揮発性メモリが複数のキーを格納し、段階（e）が前記複数のキーのそれぞれが完全に消去されるまで複数のキーのそれぞれの部分を順次消去する段階によってさらに構成される請求項1記載の方法。

5. 前記通信ユニットが非機密動作条件にない場合に、前記少なくとも1つの暗号化キーの暗号化表現を前記不揮発性メモリから消去する段階によってさらに構成される請求項1記載の方法。

6. 送信機と、受信機と、前記送信機を介して送信される情報を暗号化する暗号化手段と、前記受信機により受信される情報の暗号解読を行う暗号解読手段と、前記暗号化手段および前記暗号解読手段によって用いられ、それぞれ情報を暗号化および暗号解読する少なくとも1つのキーとを有する改善された通信ユニットであって：

前記少なくとも1つのキーの暗号化表現を格納する不揮発性メモリ手段；

前記不揮発性メモリ手段に動作可能に結合され、前記通信ユニットが機密動作条件にあるときに、前記少なくとも1つのキーの再捕捉された表現を格納する揮発性メモリ手段；

前記通信ユニットに関して非機密動作条件を検出する検

出手段；および

前記検出手段と前記揮発性メモリ手段とに動作可能に結合され、非機密動作条件が検出されると、前記少なくとも1つのキーの前記再捕捉表現を消去する消去手段；

によって構成されることを特徴とする通信ユニット。

7. 前記検出手段が、前記通信ユニットに対する電源遮断を検出する手段によりさらに構成される請求項6記載の改善された通信ユニット。

8. 前記検出手段が、前記少なくとも1つのキーに対する不当な方法によるアクセスが試みられていることを検出する手段によりさらに構成される請求項6記載の改善された通信ユニット。

9. 前記消去手段が、前記通信ユニットが非機密動作条件にないときに、前記不揮発性メモリから前記少なくとも1つのキーの前記暗号化表現を消去する手段によりさらに構成される請求項6記載の改善された通信ユニット。

【発明の詳細な説明】

暗号化通信装置内の改善された機密性に関する

方法および装置

発明の分野

本発明は、一般に暗号化通信装置に関し、特に、その改善された機密性に関する。

発明の背景

通信システムは、車内移動無線機または手持ち式携帯無線機（移動機）などの移動送信機および受信機と、基地局または中継器（固定端）などの固定送信機および固定受信機で構成されることは周知である。移動機および固定端は、別々の送信および受信通信経路により動作可能（operably）に結合される。移動機と固定端との間の通信経路は、通常は、無線周波数（R F）チャネルなどの無線リンクである。固定送信機と受信機との間の通信経路は、通常は、地上電話回線などの有線リンクである。

このような通信システム内の通常のメッセージは、移動ユニットがオーディオ信号（audio signal）を、他の移動ユニットまたは固定端へのR Fチャネル上での送信に適した

デジタル・データ・ストリームに変換することにより開始される。このようなシステムは、地方または連邦の法律執行機関などの公衆安全組織により用いられることが多い。市販の無線周波数スキャナが存在により、権限をもたない団体がこのような通信システム内で送信される情報をモニタすることが可能になる。不正な盗聴を少なくするために、通信システムはそこで送信される機密情報（proprietary information）を保護するデジタル暗号化法を用いている。

デジタル暗号化法は、既知の反転可能なアルゴリズムを用いて、デジタル・データ・ストリーム内に不規則性を取り入れる。権限をもたないユーザに対しては、暗号化されたデジタル・データ・ストリームは不規則に見えるので判読ができない。デジタル・データを不規則にするこのようなアルゴリズムをエンクリプタ（encryptor）と呼ぶ。必然的に、デジタル・データを暗号化することのできる

同じアルゴリズムが、デジタル・データ・ストリームを回復することもできなければならぬので、これはデクリプタ (decryptor) と呼ばれる。エンクリプタ／デクリプタ・アルゴリズムは、動的パラメータ (以下「キー」と呼ぶ) を利用して、デジタル・データ・ストリームに取り入れられた不規則性の性質を一意的に特定することが多い。そのため、同一のアルゴリズムおよびキーを利用するエンクリプタおよびデクリプタしか、判読可能なメッセージを再生することができない。暗号化を利用するシステムにおいては

キーの機密性が、不正なモニタを防ぐために最も重要であることは明白である。既知のエンクリプタ／デクリプタ・アルゴリズムのキーが入手されると、権限をもたない団体が専有の通信をモニタする能力が大幅に強化される。

通常、暗号化通信ユニット内では、このユニット内で用いられるキーは、RAM (ランダム・アクセス・メモリ) などの揮発性メモリ装置に格納される。この格納法により、暗号化モード・チャネルのスキャンなどの機能に必要とされる場合に、通信ユニットがキーに迅速にアクセスすることができる。また、揮発性メモリを用いることにより、通信ユニットが電力を遮断されたり、干渉 (tamper) された場合に、キー情報を消去して、機密性を維持することができる。たとえば、通信ユニットの電力が遮断されて、干渉を受けると、揮発性メモリに格納されている情報は受動的に消去される。受動的消去とは、通常、揮発性メモリ内に格納されている情報が電力を遮断されて消滅することを意味する。しかし、その後で通信ユニットに電力が供給されたときに、キーを再ロードするには外部装置が必要になる。この要件は、手持ち式携帯無線機など電力が頻繁に循環する通信ユニットにおいては煩わしい。

キー情報格納のために揮発性メモリを用いることのさらに別の欠点は、このような装置の受動的消去に信頼性がない場合が多いことである。RAM装置によっては、数分間 (場合によっては数時間) 電力が遮断されても、そこに格

納されているキー情報の一部または全部が残っているものがある。キー情報がこのように入手できる可能性があることは、通信システム全体に対する重大な機密

性の侵害につながる可能性がある。そのため、効果的でない受動的キー消去の危険を犯さずに揮発性メモリをキー格納のために使用することができ、キー消去が成功した場合には外部のキー再ロードを必要としない方法が必要になる。

図面の簡単な説明

第1図は、本発明による通信ユニットの機能ブロック図である。

第2図は、本発明による電力検知回路である。

第3図は、本発明を実行するために用いることのできる流れ図である。

好適な実施例の説明

本発明は、一般に、暗号化／暗号解読キー（キー）を格納および利用する際に、より機密性を図るための方法および装置を提供する。これは、キーの暗号化された表現をEEPROM（電氣的消去書込可能読み取り専用メモリ）などの不揮発性メモリに格納することにより達成される。通信ユニットに電源が投入されると、キーの暗号化表現が解

読されてキーを再構築し、再構築されたキーはRAMなどの揮発性メモリに格納される。RAMにキーが格納されると、通信ユニットはキーに迅速にアクセスして、情報をすばやく暗号化および暗号解読することができる。

本発明は、また、通信ユニットへの電力が遮断されたり、干渉を受けた際の、機密性を強化する。いずれの条件も、RAM内に格納されたキーを積極的に消去する。この消去手順は、各キーの一部を消去して、数マイクロ秒以内にすべてのキーが破壊されるようにすることによって順次実行される。

本発明は、第1図ないし第3図を用いて、より詳しく説明することができる。第1図は、受信機101、送信機102、デクリプタ103、エンクリプタ104、RAM105、EEPROM106、マイクロコントローラ107、電力検知回路108、デジタルーアナログ変換器109、アナログーデジタル変換器110、スピーカ111、マイクロホン112およびアンテナ113によって構成される通信ユニット100を示す。通信ユニット100は、手持ち式（hand held）移動無線機または固定端トランシーバなどの被暗号化データ送信および／または受信を必要とする任意の通信装置である。マイクロコントローラ107は、

例えばモトローラ社製68HC11K4マイクロコントローラにより構成される。デクリプタ103およびエンクリプタ104は、単独のIC装置で構成しても、別々のIC装置で

構成してもよい。

通信ユニット100の動作には、EEPROM106に格納されるキーの暗号化表現が必要とされる。通信ユニット100内で新しいキーを追加したり、既存のキーを変更する場合には、外部装置が用いられて、新しい暗号化されていないキーをRAM105内にダウンロードする。暗号化されるキー以外の既知の暗号化キー（以下マスタ・キーと呼ぶ）が、マイクロコントローラ107によりエンクリプタ104に格納される。マイクロコントローラ107は、次に、マスタ・キーとエンクリプタ104とを用いて、RAM105内に格納されているキーとマスタ・キー自身とを暗号化する。これらの被暗号化キーは、EEPROM106に格納される。電力が遮断されると、RAM105内の暗号化されていないキーが消去され、暗号化されていないマスタ・キーはデクリプタ103に格納される。次に電力が投入されたときに、マイクロコントローラ107は、デクリプタ103内のマスタ・キーがまだ有効（valid）であるかを確認する。有効でない場合は、マイクロコントローラ107により警告フラグが設定されて、通信ユニット100が干渉を受けたことを知らせる。マスタ・キーがまだ有効である場合は、マイクロコントローラ107は、既知の疑似乱数データ・ストリームをエンクリプタ104に送って、結果のキー・ストリームを回復する。マイクロコントローラ107は、このキー・ストリームを用いてEEP

ROM106内に常駐する被暗号化キーの暗号解読を行う。暗号解読されたキーは、その後RAM105内に格納されて、マイクロコントローラ107によるアクセスの便宜を図る。

RAM105内に暗号化されていないキーが格納されている状態でも、通信ユニットの通常の動作を開始することができる。暗号化音声メッセージ送信を処理するために、マイクロコントローラ107は、RAM105からエンクリプタ1

04内にキーをロードする。ユーザがマイクロホン112に向かって話しかけると、アナログーデジタル変換器110が音声信号のデジタル・データ・ストリーム表現を生成する。このデジタル・データは、マイクロコントローラ107に送られ、そこでデータはパッケージ化され、同時にエンクリプタ104に転送される。エンクリプタ104内で、DES (Data Encryption Standard: データ暗号化基準) などの既知の暗号化アルゴリズムがこのキーを利用して、データを暗号化する。マイクロコントローラ107は、エンクリプタ104から暗号化データを検索して、それを送信機102に送る。

暗号化音声メッセージの受信は、これと逆の方向に進む。マイクロコントローラ107は、RAM105からデクリプタ103内にキーをロードする。受信機101は、暗号化データをマイクロコントローラ107に送り、マイクロコントローラ107はデータをデクリプタ103に送る。

デクリプタ103内で、DESなどのデータを暗号化するために用いられたのと同じアルゴリズムが、このキーを利用してデータの暗号解読を行う。マイクロコントローラ107は、デクリプタ103から暗号解読されたデータを検索して、それをデジタルーアナログ変換器109に送る。最後に、デジタルーアナログ変換器109の出力をスピーカ111に送ることによって、音声メッセージを耳で聞くことができる。暗号化および暗号解読されるメッセージは、音声メッセージだけに制限される訳ではないことを理解されたい。テキスト・ファイルのASCII表現などのメッセージ・データも用いることができる。

RAM105とEEPROM106は、別々の部品でも、マイクロコントローラ107の一部でもよいことをさらに理解頂きたい。本発明は後者の選択肢を用いている。RAM105, EEPROM106およびマイクロコントローラ107を同じ装置内に有することの最も大きな利点は、機密性の強化である。これらのブロックをモトローラ製68HC11K4などのマイクロコントローラ107内に入れることによって、RAM105またはEEPROM106に対するすべてのアクセスは、マイクロコントローラ107を通らなければならなくなる。これを取り消そうとすると(すなわちモトローラ68HC11K4のブートストラップ・モ

ードを使おうとすると)、マイクロコントローラ107は、RAM105およびEEPROM106の内容を自動的に

消去する。他の利点としては、部品と価格の削減ならびにアクセス時間の改善があげられる。

RAM105内に暗号化されていないキーを配置し、EEPROM107内に暗号化されたキーを配置することは、本質的に機密上の危険性を招く。キーの機密性を最大限に提供するためには、敵対者(adversary)による干渉に対して通信ユニット100を保護しなければならない。これは、干渉ループおよび干渉検出回路によって行われる。干渉ループは、キー情報をもつ装置に物理的にアクセスするために破壊しなければならない電気経路である。通信ユニット100を分解したり、それに干渉しようとする、干渉回路構成がループが破壊されたことを検出する。干渉回路は、マイクロコントローラ107を起動して、デクリプタ103内に格納されるキーを消去する。通信ユニット100に現在電力が供給されていて、干渉が試みられている間に動作しているとする、マイクロコントローラ107は割込ルーチンを実行して、割込の原因を判定する。割込が干渉侵害により発生したことが判定されると、マイクロコントローラ107はすぐにRAM105内に格納されているすべてのキーを消去して、電力投入リセット・ルーチンを実行する。電力投入ルーチンにおいては、マイクロコントローラ107は、デクリプタ103に格納されるマスタ・キーの正当性をチェックする。次にマイクロコントローラ107は、デクリプタ103内のマスタ・キーが無効である

ことを判定して、マイクロコントローラ107によりエラー・フラグが設定されて、干渉が起こったことを知らせる。

通信ユニット100の電力が遮断されているときに干渉が起こると、干渉回路はデクリプタ103内に格納されているキーを消去するだけである。デクリプタ103は通信ユニット100の状態に関わらず常に電力が供給されているので、これが可能になる。結果的に通信ユニット100に電力が供給されると、マイクロコントローラ107は直ちに、デクリプタ103内に格納されているマスタ・

キーが破壊されたことを判定して、エラー・フラグが設定され、干渉侵害が起こったことを知らせる。このようなことが起こると、マイクロコントローラ107にはEEPROM106から被暗号化キーを回復するための手段がない。

干渉ループおよび干渉検出回路と共に、電力検出回路108は、電力供給移行期間または干渉検出期間中にマイクロコントローラ107が適切に動作してるか確認する。特に、電力検出回路108は、電力投入条件中にマイクロコントローラ107が正しくリセット状態から抜け出せるようにして、電力遮断または干渉条件中のリセット状態に入る前にRAM105内に格納されるすべてのキー情報をマイクロコントローラ107が消去できるようにしなければならない。

第2図は、マイクロコントローラ107に接続された電力検出回路108を示す。電力検出回路108は、低電圧

検出器200、電圧レギュレータ201、ショットキー・ダイオード202、抵抗203、204、205、被規制電圧電源(SW_+5V)206、バッテリー電圧電源(SW_B+)207、バックアップ電力キャパシタ208、マスキング不能(non-maskable)割込(XIRQb)209、リセット取り消しピン(PC7)210およびリセット入力(RESETb)211によって構成される。

低電圧検出器200は、例えばセイコー社製S-8054電圧検出器である。

電圧レギュレータ201は、例えばナショナル・セミコンダクタ社製のLP2951CM電圧レギュレータである。マスキング不能割込209、リセット取り消しピン210およびリセット入力211に関して図示されるピン名は、本発明に用いられるマイクロコントローラ107がモトローラ社製MC68HC11K4マイクロコントローラであることを前提としている。

電源投入時に、リセット入力211は被規制電圧電源206により約1.0Vまで上昇する。この時点で(バッテリー電圧電源207=1.3V)、電圧レギュレータ201のERRORb出力が低論理にセットされ、抵抗205を通じてリセット入力211をアサート(assert)し、マイクロコントローラ107をリセット状態に保持する。リセット入力211がアサートされると、整流された供給電圧(regulated voltage supply)206は、マイクロコントローラ107の下

限動作電圧よりもさらに下がる。モトローラ

ーラ社製MC68HC11K4マイクロコントローラの場合は、この下限は3Vと指定される。そのため、マイクロコントローラ107のすべてのI/Oピンは、デフォルトのリセット状態になる。このリセット状態により、マイクロコントローラ107のすべてのI/Oピンがプルアップが動作可能になった（プルアップが可能な場合）入力にデフォルト設定される。本発明は、リセット取り消しピン210が内部プルアップ装置なしに入力にリセットされた状態にデフォルト設定されることを必要として、それによりリセット取り消しピン210と電圧レギュレータ201のERRORb出力が電源投入時に競合することを防ぐ。マイクロコントローラ107としてモトローラ社製MC68HC11K4マイクロコントローラを用いている場合は、本発明の最良のモードによりポートCのピン7（PC7）をリセット取り消しピン210と指定する。これはすべてのポートCI/Oピンにプルアップ装置がないためである。リセット入力211は、整流電源電圧206が4.75Vになるまで電圧レギュレータ201のERRORb出力により低に保持される。整流電源電圧206が4.75Vになると、電圧レギュレータ201のERRORb出力は3状態（開放ドレイン装置）になり、マイクロコントローラ107は、抵抗204および抵抗205のプルアップ経路を通じてリセット状態から引き出される。これによって、マイクロコントローラ107は、その電源投入ルーチンを実行する。

電源投入ルーチンの実行中は、リセット取り消しピン210は高論理出力として設定され、それによってマイクロコントローラ107をリセット状態から抜け出させる。

電源遮断シーケンスは、バッテリー電圧電源207を除去することで始まる。整流電源電圧206は、マイクロコントローラ107の整流電源電圧206入力（VDD）に接続されたバックアップ電力キャパシタにより指数関数的に減衰を始める。バックアップ電力キャパシタ208は、整流電源電圧206がマイクロコントローラ107の下限動作電圧より下がらないうちに、マイクロコントローラ

107が動作を継続できるようにするだけの十分な電荷を蓄える。ショットキー・ダイオード202は、バックアップ電力キャパシタ208に蓄えられた電荷を分離して、この電荷が電圧レギュレータ201を通じて放電しないようにするために用いられる。バッテリー電圧電源207が4.75ボルト未満に下がると、電圧レギュレータ201のERRORb出力は低論理にアサートされる。しかし、リセット取り消しピン210は、抵抗203を通じてリセット入力211を高に保持するので、マイクロコントローラ107はリセットされない。抵抗203の値は、リセット取り消しピン210が電圧レギュレータ201のERRORb出力を取り消す際に見られる抵抗分割器の効果を最小限に抑えられるくらい小さく、リセット取り消しピン210の電流駆動機能を越えない程度に大きくなるよう選定される。ま

た、バッテリー電圧電源207が4.5Vより下がると、低電圧検出器200がマスキング不能割込209を低にして、それによりRAM105からすべてのキー情報を消去するシーケンスを開始する。マイクロコントローラ107がRAM105の消去を終了すると、リセット取り消しピン210は入力として再設定される。これにより、リセット入力211の制御は、(すでに低になっている)電圧レギュレータ201のERRORb出力に渡され、マイクロコントローラ107は直ちにリセット状態になる。

第3図は、本発明を実現するためにマイクロコントローラ107が実行する本発明の論理図を示す。ステップ300で、マイクロコントローラ107は、前述のように、暗号化されたキーをEEPROM106に格納する。その後の電源投入により、マイクロコントローラ107は、デクリプタ103と共にEEPROM106内に常駐する暗号化キーの解読を行う。これをステップ301に示す。ステップ302で、マイクロコントローラ107は、再構築されたキーをRAM105に格納し、これによりマイクロコントローラ107は通常の動作中はキーに迅速にアクセスすることができる。

通常の動作中は、ステップ303により、マイクロコントローラ107は、ユニットが電源切断(loss of power)または干渉状態などの非機密動作条件(non

-secure operating condition) にあるか否かを判断することがで

きる。ユニットが非機密条件にない場合は、流れ図はステップ304に進む。ここで、マイクロコントローラ107は、ユーザが開始したキー消去要求が行われたか否かを判定する。ユーザがこれを行うには2つの方法がある：すなわち、メニュー・コマンドを実行するか、ハードウェア・キー消去スイッチを押すかである。いずれの方法も、要求時にユニットに電源が投入されていることが必要である。要求源に関わらず、マイクロコントローラ107はRAM105およびEEPROM106内のすべてのキーを消去する。このような要求が行われなかった場合は、流れ図はステップ303に戻る。

ステップ303で、マイクロコントローラ107が、ユニットが非機密動作条件にあると判定すると、流れ図はステップ306に進み、非機密条件の性質を判定する。この非機密条件が電源遮断によるものである場合は、デクリプタ103内にマスタ・キーを格納することに加えて、マイクロコントローラ107にリセットさせる前にRAM105内のすべてのキーを消去するプロセスが実行される。これをステップ307およびステップ308に示す。ステップ308で、マイクロコントローラ107は、リセット取り消しピン210を入力に変更することにより、リセット入力211の制御を電力検知回路108に解放する。ここで電力検知回路108は、マイクロコントローラ107をリセット状態にして、これにより通信ユニット100は電

力が有効な電圧レベルに回復するまで事実上動作不能になる。

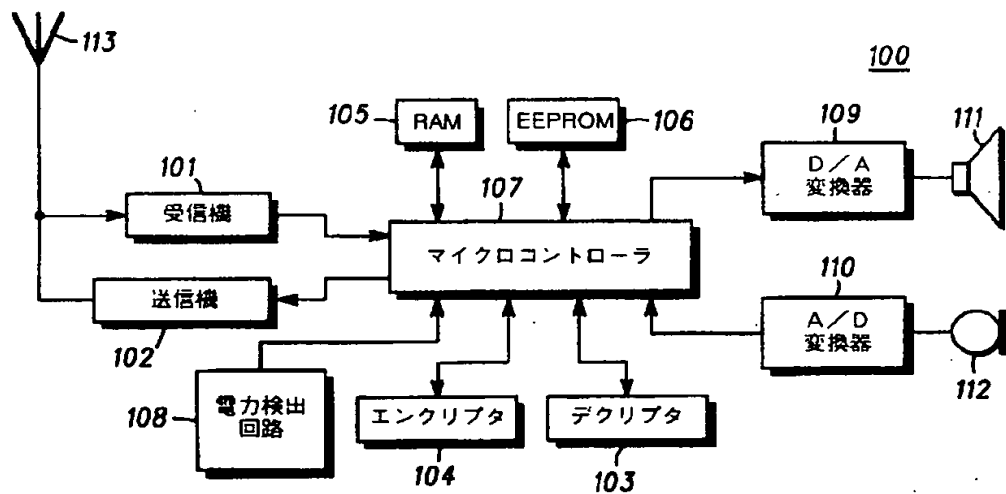
ステップ303で検出される非機密条件が電源遮断によるものでない場合は、ステップ306で、モジュールは干渉を受けていると想定される。この条件により、マイクロコントローラ107は、マスタ・キーをデクリプタ103に書き込まずにRAM105内のキーを直ちに消去する。次に、電源投入リセット動作が実行され、この間にデクリプタ103に格納されたマスタ・キーの有効性がチェックされる。マスタ・キーが破壊されたと判定されると、マイクロコントローラ107は、モジュールが干渉を受けたことを知らせるフラグを設定する。

マイクロコントローラ107は、すべてのキーができるだけ迅速に部分的に消去されるように、RAM105内のキーを積極的に消去することに注目することが重要である。まず、マイクロコントローラ107は、第1キーから、最後のキーまで進みながら、各キーの最初の2バイトを上書き（オーバーライト）する。マイクロコントローラは、すべてのキーのすべてのバイトが破壊されるまで、各キーから2バイトずつ上書きすることを続ける。

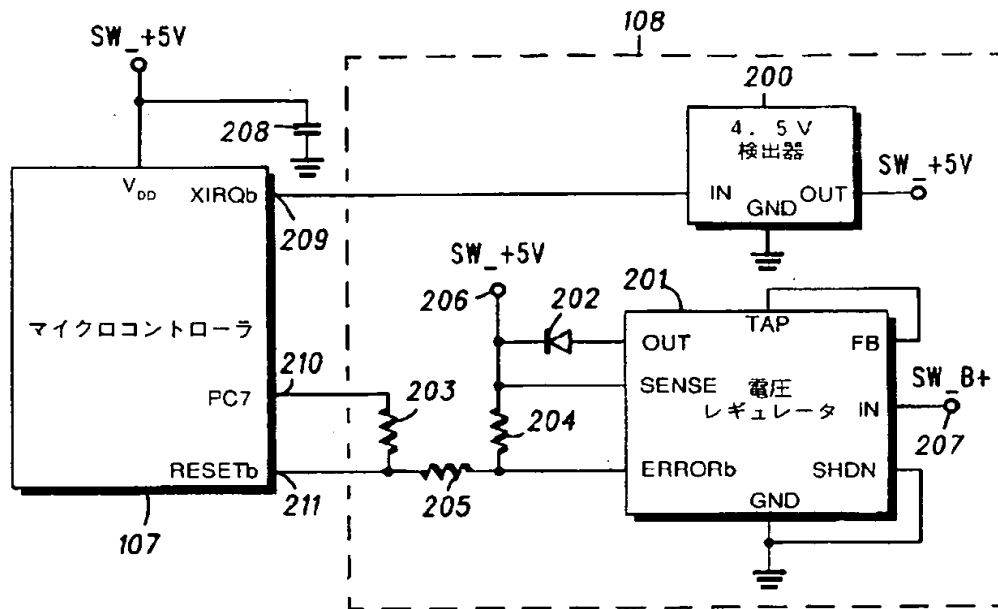
本発明は、マイクロコントローラに動作可能に結合された電力検出回路を用いて、非機密条件のときに揮発性メモリからキーを積極的に消去できるようにすることにより暗号化を利用する通信装置の機密性を改善する。本発明は、

また、不揮発性メモリにキーの被暗号化表現を格納することにより、キーが消去されるたびに揮発性メモリ内に外部からキーを再ロードする必要をなくする。

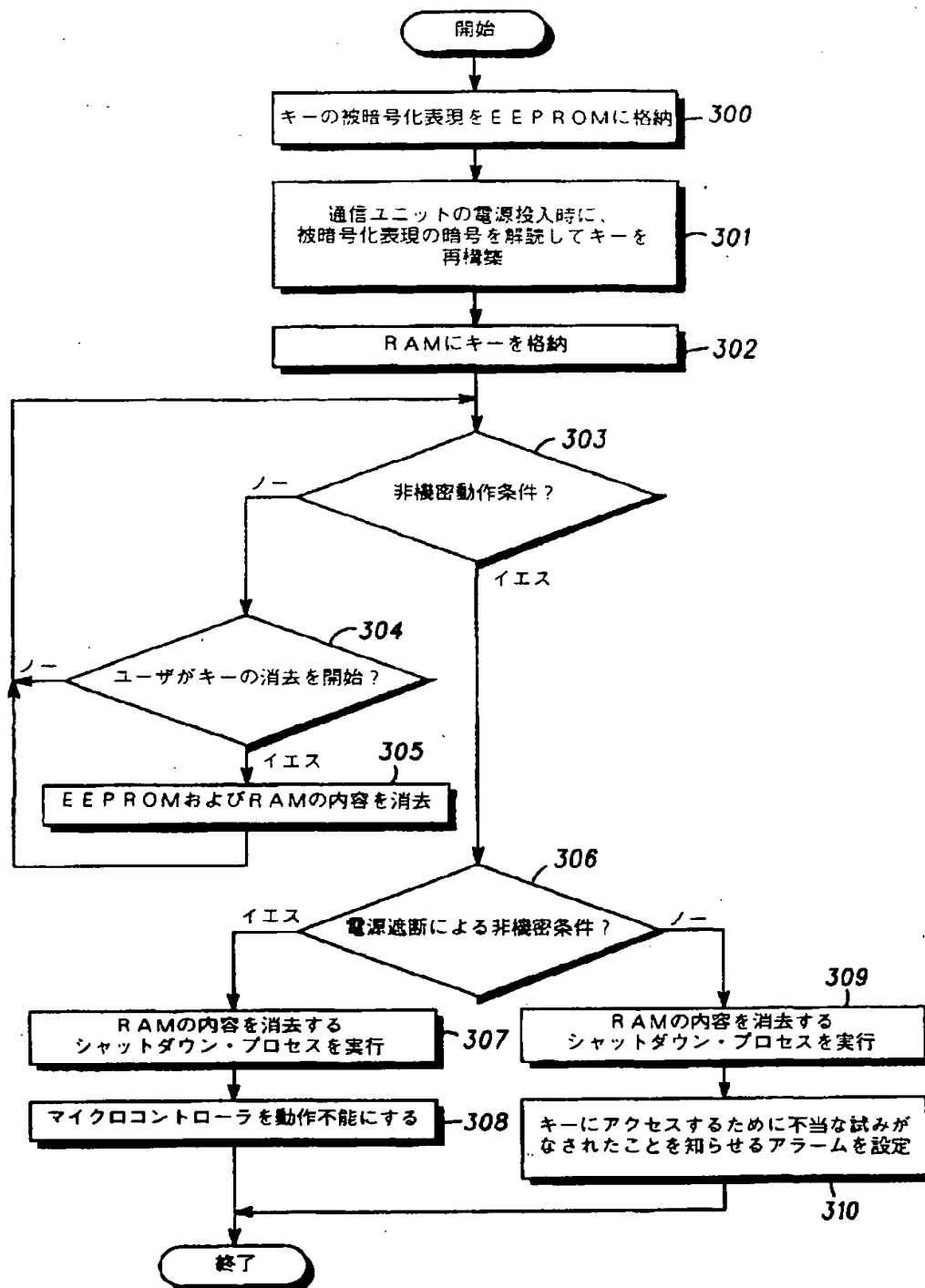
【図1】



【図2】



【図3】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US93/10914

A. CLASSIFICATION OF SUBJECT MATTER

IPCIS) : H04L 9/00

US CL : 380/4, 21, 23, 44, 45, 50

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4, 21, 23, 44, 45, 50

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,605,820 (CAMPBELL, JR) 12 AUGUST 1986, See Figs. 4-9.	1-9
Y	US, A, 4,723,283 (NAGASAWA ET AL) 02 FEBRUARY 1988, See Fig. 12B, col. 8 lines 40-45, Col. 14 lines 30-35.	1-9
A	US, A, 4,849,927 (VOS) 18 JULY 1989, See Figs. 3-4.	1-9
Y	US, A, 4,888,802 (COONEY) 19 DECEMBER 1989, See Fig. 2B, col. 4, lines 10-25.	1-9
A	US, A, 4,924,513 (HERBISON) ET AL 08 MAY 1990, See Fig. 2.	1-9

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	* T	later documents published after the international filing date or priority date and not in conflict with the application but which do not underpin the principle or theory underlying the invention
* A		document defining the general state of the art which is not considered to be part of particular relevance
* B		earlier document published on or after the international filing date
* C		document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another claim or other special reason (as specified)
* D		document referring to an oral disclosure, use, exhibition or other means
* E		documents published prior to the international filing date but later than the priority date claimed
	* X	document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
	* Y	document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
	* Z	document member of the same patent family

Date of the actual completion of the international search

07 APRIL 1994

Date of mailing of the international search report

25 APR 1994

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

SALVATORE CANGIALOSI

Telephone No. (703) 308-0482

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US93/10914

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
A	US,A, 4,926,475 (SPIOTTA ET AL) 15 MAY 1990, See Fig 1. col. 1, lines 35-45.	1-9
A	US,A 4,934,846 (GILHAM) 19 JUNE 1990, See Fig. 3.	1-9
A	US,A, 5,081,675 (KITIRUTSUNETORN) 14 JANUARY 1992, See cols. 16 and 17.	1-9
Y	US,A, 5,131,040 (KNAPCZYK) 14 JULY 1992, See entire document.	1-9
Y	US,A, 5,150,412 (MARU) 22 SEPTEMBER 1992, See Fig. 6 and cols. 1 and 2 .	1-9
A,P	US,A. 5,222,136 (RASMUSSEN ET AL) 22 JUNE 1993, See entire document.	1-9
A,P	US,A, 5,241,597 (BRIGHT) 31 AUGUST 1993, See entire document.	1-9